



# FortiManager - Release Notes

Version 6.4.5

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



January 6, 2022

FortiManager 6.4.5 Release Notes

02-645-696359-20220106

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>FortiManager 6.4.5 Release</b>	<b>6</b>
Supported models	6
FortiManager VM subscription license	6
Management extension applications	7
Supported models for MEA	7
Minimum system requirements	7
<b>Special Notices</b>	<b>8</b>
Management Extension Applications (MEA) and upgrade	8
VPN Manager in a Fabric type ADOM	8
Policy Hit Count on unused policy	8
Wireless Manager (FortiWLM) not accessible	8
SD-WAN Orchestrator not accessible	8
Support for FortiOS 6.4 SD-WAN Zones	9
FortiGuard Rating Services with FortiGate 6.4.1 or Later	9
Citrix XenServer default limits and upgrade	9
Multi-step firmware upgrades	10
Hyper-V FortiManager-VM running on an AMD CPU	10
SSLv3 on FortiManager-VM64-AWS	10
<b>Upgrade Information</b>	<b>11</b>
Downgrading to previous firmware versions	11
Firmware image checksums	11
FortiManager VM firmware	11
SNMP MIB files	13
<b>Product Integration and Support</b>	<b>14</b>
FortiManager 6.4.5 support	14
Web browsers	15
FortiOS/FortiOS Carrier	15
FortiADC	15
FortiAnalyzer	15
FortiAuthenticator	15
FortiCache	15
FortiClient	16
FortiDDoS	16
FortiMail	16
FortiSandbox	16
FortiSOAR	17
FortiSwitch ATCA	17
FortiWeb	17
Virtualization	17
Feature support	18
Language support	18

---

Supported models .....	19
FortiGate models .....	20
FortiGate special branch models .....	22
FortiCarrier models .....	22
FortiADC models .....	23
FortiAnalyzer models .....	23
FortiAuthenticator models .....	24
FortiCache models .....	25
FortiDDoS models .....	25
FortiMail models .....	25
FortiProxy models .....	26
FortiSandbox models .....	26
FortiSOAR models .....	26
FortiSwitch ATCA models .....	27
FortiWeb models .....	27
<b>Resolved Issues .....</b>	<b>29</b>
Device Manager .....	29
Others .....	29
Policy and Objects .....	30
Services .....	30
System Settings .....	30
VPN Manager .....	30
<b>Known Issues .....</b>	<b>31</b>
AP Manager .....	31
Device Manager .....	31
FortiSwitch Manager .....	33
Global ADOM .....	33
Others .....	34
Policy & Objects .....	34
Revision History .....	36
Script .....	37
Services .....	37
System Settings .....	37
VPN Manager .....	38
<b>Appendix A - FortiGuard Distribution Servers (FDS) .....</b>	<b>39</b>
FortiGuard Center update support .....	39
<b>Appendix B - Default and maximum number of ADOMs supported .....</b>	<b>40</b>
Hardware models .....	40
Virtual Machines .....	40

# Change Log

Date	Change Description
2021-02-22	Initial release.
2021-03-04	Added <a href="#">Management extension applications</a> on page 7.
2021-03-08	Updated <a href="#">Resolved Issues</a> on page 29 and <a href="#">Known Issues</a> on page 31.
2021-03-09	Updated <a href="#">Special Notices</a> on page 8.
2021-03-12	Added <a href="#">Appendix B - Default and maximum number of ADOMs supported</a> on page 40.
2021-03-18	Updated <a href="#">Appendix B - Default and maximum number of ADOMs supported</a> on page 40.
2021-03-26	Updated <a href="#">Special Notices</a> on page 8.
2021-03-30	Added <a href="#">FortiManager VM subscription license</a> on page 6.
2021-05-05	Updated <a href="#">Downgrading to previous firmware versions</a> on page 11.
2021-07-05	Updated <a href="#">Known Issues</a> on page 31.
2021-08-12	Updated <a href="#">FortiOS/FortiOS Carrier</a> on page 15.
2021-11-08	Added FMG-400G to <a href="#">Supported models</a> on page 6.
2022-01-06	Updated <a href="#">FortiMail models</a> on page 25.

# FortiManager 6.4.5 Release

This document provides information about FortiManager version 6.4.5 build 2288.



The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

- [Supported models on page 6](#)
- [FortiManager VM subscription license on page 6](#)
- [Management extension applications on page 7](#)

## Supported models

FortiManager version 6.4.5 supports the following models:

<b>FortiManager</b>	FMG-200F, FMG-300E, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E, FMG-3000F, FMG-3000G, FMG-3700F, FMG-3900E, and FMG-4000E.
<b>FortiManager VM</b>	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

## FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see [FortiManager VM firmware on page 11](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 40](#).



You can use the FortiManager VM subscription license with new FMG-VM installations. For existing FMG-VM installations, you cannot upgrade to a FortiManager VM subscription license. Instead, you must migrate data from the existing FMG-VM to a new FMG-VM with subscription license.

## Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 6.4.5.

### Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

<b>FortiManager</b>	FMG-3000F, FMG-3000G, FMG-3700F, FMG-3900E, and FMG-4000E.
<b>FortiManager VM</b>	FMG-VM64, FMG-VM64-Ali, FMG-VM64-AWS, FMG-VM64-AWSOnDemand, FMG-VM64-Azure, FMG-VM64-GCP, FMG-VM64-HV (including Hyper-V 2016, 2019), FMG-VM64-KVM, FMG-VM64-OPC, FMG-VM64-XEN (for both Citrix and Open Source Xen).

### Minimum system requirements

Some management extension applications supported by FortiManager 6.4.5 have minimum system requirements. See the following table:

Management Extension Application	Minimum system requirement
<b>SD-WAN Orchestrator</b>	At least 12GB of memory is recommended to support SD-WAN Orchestrator MEA.
<b>Wireless Manager (WLM)</b>	A minimum of 4 CPU cores and 8 GB RAM is typically required. Depending on the number of running applications, the allocated resources should be increased.

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in 6.4.5.

## Management Extension Applications (MEA) and upgrade

Upgrading FortiManager when Management Extension Applications (MEA) are enabled may reset your *System Settings* to the default settings.

To prevent your *System Settings* from being lost, please disable all Management Extension Applications (MEA) prior to upgrading FortiManager.

## VPN Manager in a Fabric type ADOM

After Upgrading to FortiManager 6.4.4, the VPN Manager may fail to install to any device participating in a full mesh VPN.

Customers using VPN Manager in a fabric type ADOM should not upgrade to 6.4.4 until the issue is resolved.

## Policy Hit Count on unused policy

FortiManager 6.4.3 and later no longer displays policy hit count information on the *Policy & Objects > Policy Packages* pane. However, you can view hit count information by using the *Unused Policies* feature and clearing the *Unused Only* checkbox. For more information, see the [FortiManager 6.4 New Features Guide](#).

## Wireless Manager (FortiWLM) not accessible

If Wireless Manager was enabled in FortiManager 6.4.0, you can no longer access it in the FortiManager GUI when you upgrade FortiManager to 6.4.2. When you try to access FortiWLM, you are redirected to the FortiManager dashboard.

## SD-WAN Orchestrator not accessible

If SD-WAN Orchestrator was enabled in FortiManager 6.4.1, you can no longer access it in the FortiManager GUI after upgrading to FortiManager 6.4.2.



To workaround this issue, run the following CLI command to manually trigger an update of SD-WAN Orchestrator to 6.4.1 r2:

```
diagnose docker upgrade sdwancontroller
```

## Support for FortiOS 6.4 SD-WAN Zones

In 6.4 ADOMs, SD-WAN member interfaces are grouped into SD-WAN zones. These zones can be imported as normalized interfaces and used in firewall policies.



Customers upgrading FortiGates from FortiOS 6.2 to 6.4 who cannot upgrade the ADOM are advised to temporarily disable SD-WAN central management until they can upgrade the ADOM to 6.4. This is to prevent FortiManager from attempting to delete the newly created SD-WAN zones on the FortiGate.

---

## FortiGuard Rating Services with FortiGate 6.4.1 or Later

FortiManager 6.4.1 or later is the supported version to provide FortiGuard rating services to FortiGate 6.4.1 or later.

## Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

### To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:  

```
xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
```
2. Confirm the setting is in effect by running `xenstore-ls`.  
-----  

```
limits = ""  
pv-kernel-max-size = "33554432"  
pv-ramdisk-max-size = "536,870,912"  
boot-time = ""
```

  
-----
3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

---

## Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

## Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

## SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol tlsv1
end
```

# Upgrade Information

You can upgrade FortiManager 6.2.0 or later directly to 6.4.5.



For other upgrade paths and details about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*.

---

This section contains the following topics:

- [Downgrading to previous firmware versions on page 11](#)
- [Firmware image checksums on page 11](#)
- [FortiManager VM firmware on page 11](#)
- [SNMP MIB files on page 13](#)

## Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. In addition the local password is erased.

A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}  
execute format {disk | disk-ext4 | disk-ext3}
```

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

## FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

## Aliyun

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

## Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

## Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

## Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

## Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FMG_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

## Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FMG_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

---

## VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information see the [FortiManager Data Sheet](#) available on the Fortinet web site. VM installation guides are available in the [Fortinet Document Library](#).

---

## SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

# Product Integration and Support

This section lists FortiManager 6.4.5 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [FortiManager 6.4.5 support on page 14](#)
- [Feature support on page 18](#)
- [Language support on page 18](#)
- [Supported models on page 19](#)

## FortiManager 6.4.5 support

This section identifies FortiManager 6.4.5 product integration and support information:

- [Web browsers on page 15](#)
- [FortiOS/FortiOS Carrier on page 15](#)
- [FortiADC on page 15](#)
- [FortiAnalyzer on page 15](#)
- [FortiAuthenticator on page 15](#)
- [FortiCache on page 15](#)
- [FortiClient on page 16](#)
- [FortiDDoS on page 16](#)
- [FortiMail on page 16](#)
- [FortiSandbox on page 16](#)
- [FortiSOAR on page 17](#)
- [FortiSwitch ATCA on page 17](#)
- [FortiWeb on page 17](#)
- [Virtualization on page 17](#)



To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```



Always review the Release Notes of the supported platform firmware version before upgrading your device.

---

## Web browsers

This section lists FortiManager 6.4.5 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 85
- Google Chrome version 88

Other web browsers may function correctly, but are not supported by Fortinet.

## FortiOS/FortiOS Carrier

This section lists FortiManager 6.4.5 product integration and support for FortiOS/FortiOS Carrier:

- 6.4.0 to 6.4.6
- 6.2.0 to 6.2.9
- 6.0.0 to 6.0.13

## FortiADC

This section lists FortiManager 6.4.5 product integration and support for FortiADC:

- 6.0.1
- 5.4.4

## FortiAnalyzer

This section lists FortiManager 6.4.5 product integration and support for FortiAnalyzer:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

## FortiAuthenticator

This section lists FortiManager 6.4.5 product integration and support for FortiAuthenticator:

- 6.0. to 6.2
- 5.0 to 5.5
- 4.3 and later

## FortiCache

This section lists FortiManager 6.4.5 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

## FortiClient

This section lists FortiManager 6.4.5 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.8
- 5.6.6
- 5.4.0 and later

## FortiDDoS

This section lists FortiManager 6.4.5 product integration and support for FortiDDoS:

- 5.4.1
- 5.3.1
- 5.2.0
- 5.1.0
- 5.0.0
- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

Limited support. For more information, see [Feature support on page 18](#).

## FortiMail

This section lists FortiManager 6.4.5 product integration and support for FortiMail:

- 6.4.0 and later
- 6.2.0 and later
- 6.0.10 and later
- 5.4.11
- 5.3.13

## FortiSandbox

This section lists FortiManager 6.4.5 product integration and support for FortiSandbox:

- 3.1.4
- 3.0.6



- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

## FortiSOAR

This section lists FortiManager 6.4.5 product integration and support for FortiSOAR:

- 6.4.0 and later
- 6.0.0 and later

## FortiSwitch ATCA

This section lists FortiManager 6.4.5 product integration and support for FortiSwitch ATCA:

- 5.2.3
- 5.0.0 and later

## FortiWeb

This section lists FortiManager 6.4.5 product integration and support for FortiWeb:

- 6.3.10
- 6.2.4
- 6.1.2
- 6.0.7
- 5.9.1
- 5.8.6
- 5.7.2
- 5.6.1
- 5.5.6
- 5.4.1

## Virtualization

This section lists FortiManager 6.4.5 product integration and support for virtualization:

- Amazon Web Services (AWS)
- Citrix XenServer 6.0+ and Open Source Xen 4.1+
- Linux KVM
- Microsoft Azure
- Microsoft Hyper-V 2008 R2/2012/2012 R2/2016
- VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0
- Nutanix AHV (AOS 5.10.5)

- Google Cloud (GCP)
- Oracle Cloud Infrastructure (OCI)
- Alibaba Cloud (AliCloud)

## Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	Reports	Logging
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiADC		✓		
FortiAnalyzer			✓	✓
FortiAuthenticator				✓
FortiCache			✓	✓
FortiClient		✓	✓	✓
FortiDDoS			✓	✓
FortiMail		✓	✓	✓
FortiSandbox		✓	✓	✓
FortiSOAR		✓		
FortiSwitch ATCA	✓			
FortiWeb		✓	✓	✓
Syslog				✓

## Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓

Language	GUI	Reports
French		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiAnalyzer Administration Guide*.

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 6.4.5.



Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

- [FortiGate models on page 20](#)
- [FortiGate special branch models on page 22](#)
- [FortiCarrier models on page 22](#)
- [FortiADC models on page 23](#)
- [FortiAnalyzer models on page 23](#)
- [FortiAuthenticator models on page 24](#)
- [FortiCache models on page 25](#)
- [FortiDDoS models on page 25](#)
- [FortiMail models on page 25](#)
- [FortiProxy models on page 26](#)
- [FortiSandbox models on page 26](#)
- [FortiSOAR models on page 26](#)
- [FortiSwitch ATCA models on page 27](#)
- [FortiWeb models on page 27](#)

## FortiGate models

Model	Firmware Version
<b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 <b>FortiGate DC:</b> FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC <b>FortiGate Hardware Low Encryption:</b> FortiGate-100D-LENC <b>FortiWiFi:</b> FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F, <b>FortiGate VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM <b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen <b>FortiGateRugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G	6.4
<b>FortiGate:</b> FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FG-60E-DSL, FortiGate-60E-POE, FortiGate-61E, FortiGate-60F, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-100F, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FG-400E, FG-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1100E, FortiGate-1101E, FortiGate-2000E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3700D, FortiGate-3800D, FortiGate-2200E, FortiGate-2201E, FortiGate-2200E, FortiGate-2201E, FortiGate-3300E, FortiGate-3301E, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	6.2

Model	Firmware Version
<p><b>FortiGate DC:</b> FortiGate-80C-DC, FortiGate-401E-DC, FortiGate-600C-DC, FortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600C-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC</p> <p><b>FortiGate Hardware Low Encryption:</b> FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC</p> <p><b>FortiWiFi:</b> FortiWiFi-30D, FortiWiFi-30D-POE, FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-80CM, FortiWiFi-81CM, FortiWiFi-60F, FortiWiFi-61F</p> <p><b>FortiGate-VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager</p> <p><b>FortiGate Rugged:</b> FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G</p> <p><b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen</p>	
<p><b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FortiGate-60F, FortiGate-61F, FG-60F, FG-61F, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FortiGate-100F, FortiGate-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FortiGate-2200E, FortiGate-2201E, FG-2500E, FortiGate-3300E, FortiGate-3301E, FG-3000D, FG-3100D, FG-3200D, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E</p> <p><b>FortiGate 5000 Series:</b> FG-5001D, FG-5001E, FG-5001E1</p> <p><b>FortiGate DC:</b> FG-401E-DC, FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3600E-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC</p> <p><b>FortiGate Hardware Low Encryption:</b> FG-100D-LENC, FG-600C-LENC</p> <p><b>Note:</b> All license-based LENC is supported based on the FortiGate support list.</p> <p><b>FortiWiFi:</b> FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D, FortiWiFi-60F, FortiWiFi-61F,</p> <p><b>FortiGate VM:</b> FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP, VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen</p> <p><b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D</p>	6.0

## FortiGate special branch models

Model	Firmware Version
<b>FortiGate:</b> FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81F, FortiGate-200F, FortiGate-201F	6.4
<b>FortiGate:</b> FortiGate-30E-3G4G-GBL, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81F, FortiGate-200F, FortiGate-201F, FortiGate-400E-Bypass, FortiGate-1800F, FortiGate-1801F, FortiGate-2600F, FortiGate-2601F, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F <b>FortiGate 6000 Series:</b> FortiGate-6000F <b>FortiGate 7000 Series:</b> FortiGate-7000E <b>FortiGate DC:</b> FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-4200F-DC, FortiGate-4201F-DC <b>FortiGate Rugged:</b> FortiGateRugged-90D <b>FortiWiFi:</b> FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ,	6.2
<b>FortiGate:</b> FortiGate-30E-3G4G-GBL, FortiGate-41F, FortiGate-41F-3G4G, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60F, FortiGate-61F, FortiGate-400E, FortiGate-401E, FortiGate-600E, FortiGate-601E, FortiGate-1800F, FortiGate-1801F, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E <b>FortiGate 6000 Series:</b> FortiGate-6000F, FortiGate-6300F, FortiGate-6301F, FortiGate-6500F, FortiGate-6501F <b>FortiGate 7000 Series:</b> FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC <b>FortiGate DC:</b> FortiGate-1100E-DC, FortiGate-3400E-DC, FortiGate-3401E-DC <b>FortiGate VM:</b> FortiGate-VM64-RAXONDEMAND <b>FortiWiFi:</b> FortiWiFi-41F, FortiWiFi-41F-3G4G,	6.0

## FortiCarrier models

Model	Firmware Version
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.4

Model	Firmware Version
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	6.2
<b>FortiCarrier:</b> FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E <b>FortiCarrier-DC:</b> FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC <b>FortiCarrier-VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	6.0

## FortiADC models

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	6.0
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	5.4

## FortiAnalyzer models

Model	Firmware Version
<b>FortiAnalyzer:</b> FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E <b>FortiAnalyzer VM:</b> FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4

Model	Firmware Version
<b>FortiAnalyzer:</b> FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E.	6.2
<b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.	6.0
<b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.	5.6
<b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.	5.4
<b>FortiAnalyzer VM:</b> FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B	5.2
<b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B	5.0
<b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	

## FortiAuthenticator models

Model	Firmware Version
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E	4.3, 5.0-5.5, 6.0
<b>FortiAuthenticator VM:</b> FAC-VM	
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-3000B, FAC-3000D, FAC-3000E	4.0-4.2
<b>FortiAuthenticator VM:</b> FAC-VM	



## FortiCache models

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E	4.0, 4.1, 4.2
<b>FortiCache VM:</b> FCH-VM64, FCH-KVM	

## FortiDDoS models

Model	Firmware Version
<b>FortiDDoS:</b> FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.2, 5.3
<b>FortiDDoS:</b> FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
<b>FortiDDoS:</b> FI-1500E, FI-2000E	5.0
<b>FortiDDoS:</b> FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.7

## FortiMail models

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.4
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.2
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM	6.0
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E	5.4
<b>FortiMail Low Encryption:</b> FE-3000C-LENC	
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B	5.3
<b>FortiMail Low Encryption:</b> FE-3000C-LENC	
<b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	

## FortiProxy models

Model	Firmware Version
<b>FortiProxy:</b> FPX-400E, FPX-2000E, FPX-4000E	1.0, 1.1, 1.2
<b>FortiProxy VM:</b> FPX-KVM, FPX-VM64	

## FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	3.1
<b>FortiSandbox-VM:</b> FSA-AWS, FSA-VM	
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	3.0
<b>FortiSandbox VM:</b> FSA-AWS, FSA-VM	
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	2.5.2
<b>FortiSandbox VM:</b> FSA-KVM, FSA-VM	
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D	2.4.1
<b>FortiSandbox VM:</b> FSA-VM	2.3.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3500D	2.2.0
<b>FortiSandbox VM:</b> FSA-VM	2.1.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D	2.0.3
<b>FortiSandbox VM:</b> FSA-VM	1.4.2
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

## FortiSOAR models

Model	Firmware Version
<b>FortiSOAR VM:</b> FSR-VM	6.4
<b>FortiSOAR VM:</b> FSR-VM	6.0

## FortiSwitch ATCA models

Model	Firmware Version
<b>FortiController:</b> FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-5913C	5.2.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B <b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B	4.3.0 4.2.0

## FortiWeb models

Model	Firmware Version
<b>FortiWeb:</b> FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.2, 6.3
<b>FortiWeb:</b> FortiWeb-100D, FortiWeb-400C, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	6.1
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER	6.0.1
<b>FortiWeb:</b> FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.9.1
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.8.6

Model	Firmware Version
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.7.2
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D <b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	5.6.1
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	5.5.6
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	5.4.1
<b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV	5.3.9
<b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E <b>FortiWeb VM:</b> FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR	5.2.4

# Resolved Issues

The following issues have been fixed in 6.4.5. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## Device Manager

Bug ID	Description
610134	FortiManager may not be able to save the admin setting page.
616387	Device configuration dashboard cannot update hostname or VDOM.
658832	FortiManager is unable to retrieve <i>priority-members</i> if outgoing interface is using the <i>Manual strategy</i> in SD-WAN rule.
659387	FortiManager should be able to provision <i>CLI-template</i> , <i>SD-WAN-template</i> , and <i>Policy Package</i> together to the model device.
684955	Customized system dashboard may disappear after awhile.
684961	Registration with NSX-T may fail with error: <i>Register service failed</i> .
688541	FortiManager should not unset <code>dynamic-vlan</code> of wireless-controller VAP and gateway of router settings after import.
688972	SD-WAN rules may lose all interface members after upgrade.
689920	FortiWeb serial number may not be correctly recognized and firmware version is not available in the <i>Add device</i> wizard.
690241	FortiManager may fail to auto-link with FortiGate with error: <i>Failed to update device management data 'invalid value - devmgmtdatafailed invalid value</i> .
696496	auto-link may fail when <i>Workspace</i> is enabled.

## Others

Bug ID	Description
667421	FortiManager may report repeated miglogd crashes which causes log lost.
671444	FortiManager may fail to check-in configuration revision with the HA secondary unit.
682404	The <code>rtmmond</code> process memory usage may increase constantly.

## Policy and Objects

Bug ID	Description
660483	IPS signatures may not match between FortiGate and FortiManager.
677385	IPS profile may not load.
686591	FortiManager may not be able to add individual VWP interface members to multicast policy.
688589	Setting the <i>Local Webfilter Category Action</i> to <i>Allow</i> should not disable the action when installed on FortiGate.
690509	FortiManager may fail to install ACI-Direct connector to FortiGate due to <code>server-list</code> command.

## Services

Bug ID	Description
677875	Scheduling firmware upgrades may cause <code>fds_svrd</code> to consume 100% CPU resource.
694903	Some firmware upgrade paths may have issues.

## System Settings

Bug ID	Description
690921	ADOM upgrade from 6.0 to 6.2 should not add custom <i>ssl-ssh-profile</i> to policies which were not configured for SSL inspection.

## VPN Manager

Bug ID	Description
685704	After upgrading FortiManager, installing to any device participating in the full mesh VPN may fail with copy error <i>fetch device/vdom list failed</i> .

# Known Issues

The following issues have been identified in 6.4.5. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

## AP Manager

Bug ID	Description
633171	There may be DFS Channel mismatch between FortiManager and FortiGate for FAP-223E.
648812	DHCP server is incorrectly created for Bridge SSID.
674636	<i>SSID may be empty on AP Manager &gt; WiFi Profiles &gt; SSID column.</i>

## Device Manager

Bug ID	Description
485037	<i>Monitor &gt; Map</i> view may fail if proxy is enabled.
545239	After adding FortiAnalyzer fabric ADOM to FortiManager, <i>Device Manager's</i> log status, <i>Log Rate</i> , or <i>Device Astore</i> column cannot get data from FortiAnalyzer.
554241	FortiManager cannot delete and reassign ports to VDOM when split VDOM is enabled.
563690	Device Manager fails to add FortiAnalyzer which contains a FortiGate HA device with error: <i>Serial number does not match database</i> .
575215	When creating a new interface for a VDOM, FortiManager may list interfaces that may belong to another ADOM.
596711	FortiManager CLI Configuration shows incorrect default wildcard value for router access-list.
598431	Install wizard may show a blank area when scrolling down the wizard to select device(s).
604125	FortiManager may not be able to edit VDOM link interface from VDOM level.
610568	FortiManager may not follow the order in CLI Script template.
615044	Configuration status may be shown as <i>modified</i> after adding FortiGate to FortiManager.
624325	Creating or editing transparent VDOM to disable may get stuck at 20%.
630316	After auto-conf IPv6 address is changed on FortiGate, the address is not updated in the device database.

Bug ID	Description
636357	Retrieve may fail on FortiGate cluster with <i>Failed to reload configuration. invalid value</i> error.
636638	Fabric view may get stuck at loading.
640907	FortiManager is unable to configure FortiSwitch port mirroring.
651560	SD-WAN monitor may get stuck loading when an admin user belongs to a device group.
652052	FortiManager may fail to add another FortiManager in Fabric ADOM.
659981	FortiManager should be able to identify and show default SSL-SSH profile as <i>read-only</i> profiles.
660491	<i>Device Manager</i> system interface should not allow duplicated secondary IP address.
665207	FortiManager needs IPv6 support on Syslog server setting.
665955	FortiManager is not reflecting proper admin timeout value in CLI only object.
666872	<i>BGP Neighbors</i> table does not have height limit and vertical scrollbar.
667738	GUI should generate error message when using invalid IP address or special characters in interface name.
670535	Install fails when creating a new DHCP reservation due to missing MAC address.
670577	When creating an API admin from CLI Configuration, <i>trusted host</i> section is missing.
673548	FortiManager may not be able to make any changes to the FortiGate interface settings when the interface type is <i>Software Switch</i> .
674123	<i>SD-WAN template &gt; SD-WAN Rules</i> options for <i>Load Balance Mode</i> do not match those on FortiOS.
674904	FortiManager may not be able to import policy with interface binding contradiction on <i>srcintf</i> error.
676002	FortiManager is not re-installing a policy when the user selects all devices with VDOMs from <i>Device Manager</i> .
678495	FortiManager <i>VPN L2TP</i> may prompt <i>invalid ip range</i> .
680516	<i>Host Name</i> is truncated when name has more than 31 characters.
681627	FortiManager is accepting DNS source IP even though it is not part of the available interfaces.
683411	FortiManager may not display a FortiGate under the <i>Device Manager &gt; Managed Devices</i> .
684372	When using VDOMs, <i>Policy Package</i> status remains in modified status after using <i>Push to device</i> .
684462	FortiManager truncates the device configuration when downloading from <i>View configuration</i> option.
689014	FortiManager may return an error when changing FortiGate device log configuration from FortiManager with management VDOM is moved to another VDOM.
689721	When changing FortiGuard related settings via CLI Configuration, FortiManager shows



Bug ID	Description
	changes are reverted back but it also show the message: <i>Successfully updated</i> .
690493	License check setting may not be saved.
690566	Changed to the <i>Disclaimer Page</i> may not be saved with error.
690608	Duplicate entries for FortiExtenders may exist with same serial number.
692669	Browser may display a message, <i>A webpage is slowing down your browser</i> , while checking revision difference.

## FortiSwitch Manager

Bug ID	Description
667703	After adding FortiSwitch, running a script to provision may fail.
674539	FortiManager may fail to upgrade two FortiSwitch devices at the same time.
676739	FortiManager may not be able to delete VLAN interfaces created by FortiSwitch Manager.
690995	FortiSwitch Manager should not install the <i>auto-detected</i> setting to FortiGate.

## Global ADOM

Bug ID	Description
662216	In Global ADOMs the <i>Where Used</i> tool may not show object usage in ADOM.
667197	User should not be able to delete global object when ADOM is not locked.
680798	FortiManager may return error, <i>Could not read zone validation results</i> , when assigning global ADOM changes with <i>Automatically Install Policies to ADOM Devices</i> .
689965	Replacement message type UTM is not being pushed from global ADOM to local ADOM.
691562	Threat feeds global objects are not installed to destination ADOM when using the <i>Assign All</i> object option.
693510	Display Options for <i>Object Config</i> will reset to default after sometimes.

## Others

Bug ID	Description
510508	FortiManager cannot assign multiple ADOMs to an admin user via JSON API.
605560	Flag <i>is_model</i> and <i>linked_to_model</i> are not working when adding model device with JSON API.
667442	FortiManager may not be able to connect to FortiGate CLI via <i>SSH</i> widget or execute TCL scripts.
678322	Rebuilding database may never start when FortiAnalyzer mode is enabled.
680806	GUI access for multiple administrators may hang when upgrading multiple FortiGate devices.
681625	The <i>svc cdb</i> reader process may crash during ADOM upgrade.
681707	The <i>diagnose cdb upgrade check +a1659981</i> command may unset <i>defmap-intf</i> .
683841	FortiManager databases may randomly lose integrity.
686460	ADOM integrity check may run slowly and it takes several minutes to response for each ADOM.

## Policy & Objects

Bug ID	Description
538057	The "OR" button in column filter may not work.
580880	FortiManager is unable to see dynamic mapping for <i>Local Certificate</i> if workflow session is created.
585177	FortiManager is unable to create VIPv6 virtual server objects.
593072	After a non super user deleted a device, "super_user" admin cannot edit zone or interface with the deleted device's dynamic mappings.
601696	FortiManager may add unexpected IPv6 address to IPv6 address field when deleting <i>: / 0</i> .
607628	After deletion, creating another DNS Filter object with the same name and "Domain Filter Subtable" returns a duplicate error.
608535	<i>NAT</i> option is missing from <i>Central NAT</i> policy package.
615624	Firewall policy and proxy policy cannot select IP type external resource as address.
617894	FortiManager is missing IPV6 <i>none</i> values after modifying policy.
623100	FortiManager is constantly changing UUID for firewall address object.
630431	Some application and filter overrides are not displayed in the GUI.

Bug ID	Description
631158	FortiManager is unable to import firewall objects of <code>fssso fortiems-cloud</code> user due to Server cannot be empty.
646329	Policy Check may claim that different IPS profiles as duplicate.
652753	When an obsolete internet service is selected, FortiManager may show entry IDs instead of names.
655601	FortiManager may be slow to add or remove a URL entry on web filter with a large list.
656991	FortiManager should not allow VIP to be created with same IP for External IP and Mapped IP Address.
659296	FortiManager may take a lot of time to update web filter URL filter list.
663109	FortiManager should not allow user to select a profile group in a flow-based policy that uses a proxy-based feature.
666258	User should not be able to create a firewall policy with an Internet service with <i>Destination</i> direction in <i>Source</i> by using drag and drop.
670061	FortiManager does not report error when an unsupported FQDN address format is created.
675509	FortiManager may randomly set IPv4 IP Pool object to overload.
677528	Address object search may not display the address group which contains the searched object within the group.
679282	Editing a global object in an ADOM is not possible generating error, <i>undefined is not iterable</i> .
681006	<i>Domain Name</i> and <i>FortiGuard Category Threat Feeds</i> are not installed when set as <i>Allow</i> action in security profiles.
681453	Copy fails for address and group from the exempt list of an SSL profile not used in the policy package.
682356	FortiManager may not be able to map normalized interface.
683167	<i>Policy Package</i> single entry change may impact all <i>Policy Package Installation Targets</i> status.
684081	<i>Policy Check</i> and <i>Find Unused Policies</i> may not work for FortiGate in <i>Policy-Based</i> mode.
686902	FortiManager may not be able to configure <code>ipv4-split-exclude</code> attribute via CLI Object.
686911	Workflow session may not be able to compare with error: <i>Cannot compare because of invalid Revision Diff data</i> .
686962	FortiManager is not allowed to rename application control profile.
687460	The same filter may behave differently between source address and destination address.
687784	FortiManager may not be able to add rule with ISDB object when a rule is created with add above or below option.
689589	<i>Internet Services</i> may not match between FortiManager and FortiGate.
690269	Newly imported Cisco ACI connector object does not appear for selection until browser is refreshed.

Bug ID	Description
692114	<i>Where Used</i> returns <i>No Record Found</i> when <i>IPS Custom Signature</i> is being used.
694605	FortiManager may not be able to push the entire <i>Azure SDN Connector</i> configuration.
673554	FortiManager should not allow policy to set destination address with a Virtual Server when inspection-mode is set as "flow".

## Revision History

Bug ID	Description
606737	User may not be able to install policy package due to change with external interface with VIP settings.
618305	FortiManager changes configuration system csf settings.
623159	Zone validation in <i>Re-Install Policy</i> is not saving the user choice and deleting all related policies.
635957	Install fails for subnet overlap IP between two interfaces.
664284	FortiManager may not be able to configure SSH certificate.
671481	FortiManager may unset inspection-mode for 6.2 FortiGates in 6.0 ADOM while installation.
672609	After import, FortiManager may prompt password error on administrator during install.
674094	FortiManager may unset explicit proxy's HTTPS and PAC ports and change the value to 0 instead.
675867	The <code>ssl-anomaly-log</code> configuration may be incorrectly pushed by FortiManager when installing 5.6 ADOM policy to 6.0 FortiGate.
679139	When a policy package is shared between many firewalls, web rating override purge may fail in some scenarios.
687769	FortiManager may not be able to set <code>auto-asic-offload</code> to disable.
689270	The following attributes under <code>configs vpn ssl</code> setting may have invalid range: <code>login-attempt-limit</code> , <code>login-block-time</code> , <code>http-request-header-timeout</code> , <code>http-request-body-timeout</code> and <code>router bgp keep-alive-timer</code> .
691835	FortiManager should be able to move one VLAN to a different zone without deleting many rules or zones.
693225	FortiManager may install <code>unset inspection-mode</code> to FortiGate 6.2 device in 6.0 ADOM.
694380	Installation may fail when <code>set whitelist enable</code> in <code>ssl-ssh-profile</code> is pushed to FortiGate 6.2 from a in 6.0 ADOM.

## Script

Bug ID	Description
613575	After script is run directly on CLI, FortiManager may fail to reload configuration.
668876	Using CLI script to create SD-WAN with auto-numbering, 'edit 0', may not work.
668947	Changes using CLI script may not be applied to devices in the container or folder.
671998	TCL scripts may not work when <code>ssh-kex-sha1</code> and <code>ssh-mac-weak</code> are not enabled on FortiGate.

## Services

Bug ID	Description
567664	HA secondary device does not update FortiMeter license.
616703	GUI CLI Console may not response.
617601	Sort by Time Used in task monitor may not be correct.
680857	FortiExtender, FortiAP, or FortiSwitch upgrades can fail due to custom image being deleted during or after a failed upgrade.

## System Settings

Bug ID	Description
517964	FortiManager may crate incorrect certificate and it cannot be deleted.
579964	FMGVM64-Cloud needs to provide GUI support for ADOM upgrade in system information dashboard.
598194	FortiManager two-factor authentication admin login is missing the option for <i>FTK Mobile</i> push notification authentication.
614127	FortiManager should show details in the <code>fnbamd</code> debug if login fails due to trusted hosts.
625683	Changes made by ADOM upgrade may not update <i>Last Modified</i> date/time and user admin.
635181	FortiManager is unable to delete mail server with error message <i>used</i> displayed.
652417	FortiManager HA may go out of synchronization periodically based on the logs.
660130	Invalid setting of <code>ssl-exempt</code> may cause ADOM upgrade to fail.
670497	After upgrading FortiManager, syslog configuration may be deleted.

Bug ID	Description
684907	Changing of <i>FortiGuard Server Location</i> in <i>License Information Dashboard</i> may not have any effect.
686569	Creating and deleting the static route may remove specific connected route.
687171	Users may not be able to assign devices to the ADOMs to which they have full access.
687223	Users may not be able to upgrade ADOM because of <i>profile-protocol-options</i> .
687968	FortiManager should not change to <i>ipv6-autoconf</i> to disable when management access is changed to the <i>ipv6-autoconf</i> enable state.
688517	Upgrading ADOM may fail due to FortiExtender Object.
695058	Radius response packets should not timeout with less of the <i>remoteauthtimeout</i> setting.
699185	If Management Extension Applications are enabled, all system settings may be lost after upgraded FortiManager. <b>Workaround:</b> Please disable all Management Extension Applications (MEA) prior to upgrade.

## VPN Manager

Bug ID	Description
681110	VPN manager may not push any configuration on ADOM 6.0 for dial up VPN on FortiGate.

## Appendix A - FortiGuard Distribution Servers (FDS)

In order for the FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as a FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the items listed below:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through via port 443.

### FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform/version:

Platform	Antivirus	WebFilter	Vulnerability Scan	Software
FortiClient (Windows)	✓	✓	✓	✓
FortiClient (Mac OS X)	✓		✓	
FortiMail	✓			
FortiSandbox	✓			
FortiWeb	✓			



To enable FortiGuard Center updates for FortiMail version 4.2 enter the following CLI command:

```
config fmupdate support-pre-fgt-43
set status enable
end
```

## Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

### Hardware models

The following table identifies the default number of ADOMs supported for FortiManager hardware models G series and later. It also identifies the hardware models that support the ADOM subscription license and the maximum number of ADOMs supported.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
FMG-3000G Series	500	✓	1200

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the [FortiManager Data Sheet](#).

### Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Licenses are non-stackable. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the [FortiManager Data Sheet](#).





**FORTINET®**



Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.